(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 septembre 2005 (01.09.2005)

PCT

(10) Numéro de publication internationale
WO 2005/081452 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2005/000158

(22) Date de dépôt international :
24 janvier 2005 (24.01.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0450129 23 janvier 2004 (23.01.2004) FR

(71) Déposants *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **MATH RIZK** [BE/BE]; SPRL, Verte Voie 20, Boîte 5, B-1348 Louvain-La-Neuve (BE).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **GUILLOU, Louis** [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR). **QUISQUATER, Jean-Jacques** [BE/BE]; 3, avenue des Canards, B-1640 Rhode Saint-Genèse (BE).

(74) Mandataire : **MUSTAKI, Daniel**; France Telecom, Division R & D/PIV/PI, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :
— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour toutes les désignations*
— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** ZERO-KNOWLEDGE PROOF CRYPTOGRAPHY METHODS AND DEVICES

(54) **Titre :** PROCEDES ET DISPOSITIFS CRYPTOGRAPHIQUES SANS TRANSFERT DE CONNAISSANCE

(57) **Abstract:** A cryptography method using a key holder having a number $m = 1$ of private keys $Q_1, Q_2, , Q_m$ and respective public keys $G_1, G_2, , G_m$, where each key pair (Q_i, G_i) (where $i = 1, , m$) fits either the equation $G_i = Q_i^v \bmod n$, or the relation $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f private prime factors (where $f > 1$), denoted by $p_1, \ldots, p_f$, of which at least two are different, and exponent v is a public integer equal to a power of 2. In particular, the invention teaches the mathematical structure that can be imparted to the public keys in order to make it impossible to calculate said private keys (within a reasonable amount of time) on the basis of the public parameters, unless the prime factors are known. The invention further relates to various devices for carrying out the method.

(57) **Abrégé :** L'invention concerne un procédé de cryptographie mettant en jeu un détenteur de clés possédant un nombre $m \geq 1$ de clés privées $Q_1, Q_2, \ldots, Q_m$ et de clés publiques respectives $G_1, G_2, \ldots, G_m$, chaque paire de clés (Q_i, G_i) (où $i=1, \ldots, m$) vérifiant soit la relation $G_i = Q_i^v \bmod n$, soit la relation $G_i \times Q_i^v = 1 \bmod n$, où n est un entier public égal au produit de f facteurs premiers privés (où $f > 1$), notés $p_1, \ldots, p_f$, dont deux au moins sont distincts, et l'exposant v est un entier public égal à une puissance de 2. L'invention enseigne notamment quelle structure mathématique on peut donner aux clés publiques de manière à ce qu'il soit impossible, à partir desdits paramètres publics, de calculer (en un temps raisonnable) lesdites clés privées, à moins de connaître lesdits facteurs premiers. L'invention concerne également divers dispositifs destinés à mettre en œuvre ce procédé.

WO 2005/081452 A1